PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-116534
(43)Date of publication of application : 02.05.1997

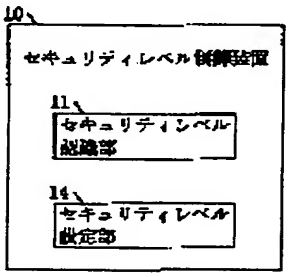
(51)Int.Cl. H04L 9/32
G06F 13/00
G06F 15/00
H04L 9/14

(21)Application number : 07-271578
(22)Date of filing : 19.10.1995

(71)Applicant : FUJITSU LTD
(72)Inventor : KURODA YASUTSUGU

(54) SECURITY LEVEL CONTROLLER AND NETWORK COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To conduct communication without deciding a security level in advance with a communication destination by providing a security level setting section that sets a security level recognized by a security level recognition section as a security level at a security level controller.
SOLUTION: A security level controller 10 is provided with a security level recognition section 11 and a security level setting section 14. The security level recognition section 11 recognizes a security level informed by a communication destination. The security level setting section 14 sets the security level recognized by the security level recognition section 11 as a security level of the security level controller 10. Then the security level of the communication destination recognized by the security level recognition section 11 is set for the security level of the security level controller 10.



LEGAL STATUS

[Date of request for examination] 29.08.2001
[Date of sending the examiner's decision of rejection] 17.08.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2004-19344
[Date of requesting appeal against examiner's decision of rejection] 16.09.2004

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－116534

(43)公開日　平成９年(1997)５月２日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７３Ｂ
Ｇ０６Ｆ	13/00	３５７		Ｇ０６Ｆ	13/00	３５７Ｚ
	15/00	３３０			15/00	３３０Ａ
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１

審査請求　未請求　請求項の数12　ＯＬ　（全 17 頁）

(21)出願番号　特願平7－271578

(22)出願日　平成７年(1995)10月19日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　遠山　勉　（外１名）

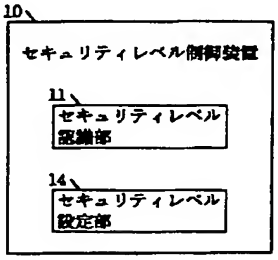
(54)【発明の名称】　セキュリティレベル制御装置及びネットワーク通信システム

(57)【要約】

【課題】　通信先との間で予めセキュリティレベルを決定しておくことなく、通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第１の課題とする。

【解決手段】　セキュリティレベル制御装置は、通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部１１と、セキュリティレベル認識部１１で認識されたセキュリティレベルをセキュリティレベル制御装置１０側のセキュリティレベルとして設定するセキュリティレベル設定部１４とを備えて構成した。

本発明の第１のセキュリティレベル制御装置に対応した原理ブロック図



【特許請求の範囲】
【請求項１】　通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置において、
通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、
前記セキュリティレベル認識部で認識されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを備えたことを特徴とするセキュリティレベル制御装置。
【請求項２】　通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置において、
通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、
２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、
前記セキュリティレベル認識部で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部と、
前記セキュリティレベル読出部から読み出されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを備えたことを特徴とするセキュリティレベル制御装置。
【請求項３】　セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、
前記クライアント装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、
通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、
前記セキュリティレベル認識部で認識されたセキュリティレベルを前記クライアント装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを特徴とするネットワーク通信システム。
【請求項４】　セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、
前記サーバ装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、
通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、
前記セキュリティレベル認識部で認識されたセキュリティレベルを前記サーバ装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを特徴とするネットワーク通信システム。
【請求項５】　前記サーバ装置は複数設けられており、前記クライアント装置に設けられた前記セキュリティレベル制御装置は、各々のサーバ装置毎にセキュリティレベルを制御することを特徴とする請求項３に記載のネットワーク通信システム。
【請求項６】　前記クライアント装置は複数設けられており、
前記サーバ装置に設けられた前記セキュリティレベル制御装置は、各々のクライアント装置毎にセキュリティレベルを制御することを特徴とする請求項４に記載のネットワーク通信システム。
【請求項７】　前記クライアント装置が有する前記セキュリティレベル制御装置は、
２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、
前記セキュリティレベル認識部で認識された前記サーバ装置のセキュリティレベル及び前記クライアント装置のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部とを有し、
前記セキュリティレベル設定部は、前記セキュリティレベル読出部から読み出されたセキュリティレベルを前記クライアント装置側のセキュリティレベルとして設定することを特徴とする請求項３又は請求項５に記載のネットワーク通信システム。
【請求項８】　前記サーバ装置が有する前記セキュリティレベル制御装置は、
２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、
前記セキュリティレベル認識部で認識された前記クライアント装置のセキュリティレベル及び前記サーバ装置のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部とを有し、
前記セキュリティレベル設定部は、前記セキュリティレベル読出部から読み出されたセキュリティレベルを前記サーバ装置側のセキュリティレベルとして設定することを特徴とする請求項４又は請求項６に記載のネットワーク通信システム。
【請求項９】　前記クライアント装置が有する前記セキュリティレベル制御装置は、前記クライアント装置の要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項７に記載のネットワーク通信システム。
【請求項１０】　前記サーバ装置が有する前記セキュリ

ティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項８に記載のネットワーク通信システム。

【請求項１１】　セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、

前記サーバ装置及び前記クライアント装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、

前記セキュリティレベル認識部で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部と、

前記セキュリティレベル読出部から読み出されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを特徴とするネットワーク通信システム。

【請求項１２】　前記クライアント装置が有する前記セキュリティレベル制御装置は、前記クライアント装置の要求に従って、通信途中でも、セキュリティレベルを動的に変化させ、

前記サーバ装置が有する前記セキュリティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項１１に記載のネットワーク通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティレベル制御装置、特に通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置に関する。

【０００２】また、本発明は、ネットワーク通信システム、特にセキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムに関する。

【０００３】

【従来の技術】分散して設置されている計算機を相互に接続することにより、電子メール等のサービスを提供するネットワークサービスが商用化されている。

【０００４】ところが、インターネットに代表されるように学術目的で構築されてきたネットワークでは、ネットワークセキュリティに関する考慮が十分にされていない。そのため、ネットワークサービスに対して盗聴、改竄、なりすまし等が行われ問題となっている。

【０００５】ここで、電子メールを例に取り、盗聴、改竄、なりすましについて説明する。盗聴とは、平文、即ち何も暗号化されていない状態の通信文（メッセージ）が配送途中で読まれてしまうことをいう。

【０００６】改竄とは、配送途中で電子メールの内容が変更されてしまうことをいう。改竄は、電子メールが複数の中継ノードを経由して配送される場合に、途中の中継ノードで行われる。

【０００７】なりすましとは、発信者を特定する情報が保護されていない場合に、悪意を持つ第三者が発信者情報を偽造して他人になりすますことをいう。このような問題を解決するため、メッセージ（データ）を暗号化すること、電子署名を用いて改竄を防ぐこと、ユーザ（通信相手）を認証することなどが単独あるいは組み合わされて行われている。また、サーバ及びクライアントの形態を持つネットワーク通信では、サーバ装置を認証することやクライアント装置を認証することも行われている。

【０００８】ここで、暗号化技術としては、秘密鍵暗号方式や公開鍵暗号化方式等が知られている。秘密鍵暗号化方式では、通信の当事者間で共通の鍵を使って暗号化と復号化を行う。一方、公開鍵暗号化方式は、各人の秘密鍵と公開鍵の組み合わせで構成され、他者には公開鍵を知らせ、秘密鍵は自分一人だけが知っている方式である。この方式では、公開鍵で暗号化されたものは秘密鍵で解くことができる。例えば、ＡからＢへ送信するときには、ＡはＢの公開鍵で暗号化を行い、受け取ったＢは自分の秘密鍵でこれを解く。この暗号文を解けるのは、自分の秘密鍵を知るＢだけである。

【０００９】また、認証技術については、パスワード認証、公開鍵方式を用いた電子署名等が知られている。

【００１０】

【発明が解決しようとする課題】前記従来の技術において、ネットワークサービスに対して盗聴、改竄、なりすまし等を防止するため、どのような処理を組み合わせるかにより、複数のセキュリティレベルが生じることになる。

【００１１】例えば、電子メールを暗号化することだけよりも、電子メールを暗号化すると同時にユーザ認証を行う方がセキュリティレベルが高いと考えられる。セキュリティを強化することだけを考えれば、より多くの処理を組み合わせた方が安全ではあるが、その場合に負荷が高くなるのも事実である。

【００１２】そこで、通信内容の重要性を反映させたセキュリティレベルを設定することが適切であると考えられるが、メッセージの重要性に基づいて適切なセキュリティレベルを設定することを「セキュリティのポリシ

一」という。

【００１３】ところで、前記従来の技術においては、この「セキュリティのポリシー」に関して下記のような問題が生じている。第１の問題は、通信先との間で予め決められたセキュリティのポリシーでしか通信できず、それ以外のポリシーでは通信できないことである。

【００１４】第２の問題は、通信先のセキュリティレベルが常に優先され、自分のセキュリティレベルを反映できないことである。本発明は、このような事情に鑑みてなされたもので、通信先との間で予めセキュリティレベルを決定しておくことなく通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第１の課題とする。

【００１５】また、本発明は、自分のセキュリティレベルを反映させた通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第２の課題とする。

【００１６】

【課題を解決するための手段】

《本発明の第１のセキュリティレベル制御装置１０》本発明の第１のセキュリティレベル制御装置１０は、前述した第１の課題を解決するため以下のように構成されている（請求項１に対応）。図１は、本発明のセキュリティレベル制御装置１０に対応した原理ブロック図である。

【００１７】即ち、通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置１０において、セキュリティレベル認識部１１及びセキュリティレベル設定部１４を備えて構成されている。

【００１８】（セキュリティレベル認識部１１）前記セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。

【００１９】（セキュリティレベル設定部１４）前記セキュリティレベル設定部１４は、前記セキュリティレベル認識部１１で認識されたセキュリティレベルをセキュリティレベル制御装置１０側のセキュリティレベルとして設定する。

【００２０】本発明の第１のセキュリティレベル制御装置１０によれば、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識された通信先のセキュリティレベルが、セキュリティレベル制御装置１０側のセキュリティレベルとして設定される。

【００２１】《本発明の第２のセキュリティレベル制御装置１０》本発明の第２のセキュリティレベル制御装置１０は、前述した第２の課題を解決するため以下のように構成されている（請求項２に対応）。図１は、本発明のセキュリティレベル制御装置１０に対応した原理ブロック図である。

【００２２】即ち、通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置１０において、セキュリティレベル認識部１１、セキュリティレベル変換テーブル部１２、セキュリティレベル読出部１３及びセキュリティレベル設定部１４を備えて構成されている。

【００２３】（セキュリティレベル認識部１１）前記セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。

【００２４】（セキュリティレベル変換テーブル部１２）前記セキュリティレベル変換テーブル部１２は、２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【００２５】（セキュリティレベル読出部１３）前記セキュリティレベル読出部１３は、前記セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置１０側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部１２から読み出す。

【００２６】（セキュリティレベル設定部１４）前記セキュリティレベル設定部１４は、前記セキュリティレベル読出部１３から読み出されたセキュリティレベルをセキュリティレベル制御装置１０側のセキュリティレベルとして設定する。

【００２７】本発明の第２のセキュリティレベル制御装置１０によれば、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置１０側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部１２から読み出される。そして、この読み出されたセキュリティレベルがセキュリティレベル装置１０側のセキュリティレベルとして設定される。

【００２８】《本発明の第１のネットワーク通信システム》本発明の第１のネットワーク通信システムは、前述した第１の課題を解決するため以下のように構成されている（請求項３に対応）。図３は、本発明の第１のネットワーク通信システムに対応した原理ブロック図である。

【００２９】即ち、セキュリティレベルが設定された通信を行うサーバ装置２０及びクライアント装置３０が設けられたネットワーク通信システムにおいて、前記クライアント装置３０は、セキュリティレベル制御装置１０を有する。そして、このセキュリティレベル制御装置１０は、セキュリティレベル認識部１１及びセキュリティレベル設定部１４を備えて構成されている。

【００３０】（セキュリティレベル認識部１１）前記セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。

【００３１】（セキュリティレベル設定部１４）前記セキュリティレベル設定部１４は、前記セキュリティレベル認識部１１で認識されたセキュリティレベルを前記クライアント装置３０側のセキュリティレベルとして設定する。

【００３２】本発明の第１のネットワーク通信システムによれば、クライアント装置３０側において、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識されたサーバ装置２０のセキュリティレベルが、クライアント装置３０側のセキュリティレベルとして設定される。

【００３３】《本発明の第２のネットワーク通信システム》本発明の第２のネットワーク通信システムは、前述した第１の課題を解決するため以下のように構成されている（請求項４に対応）。図４は、本発明の第２のネットワーク通信システムに対応した原理ブロック図である。

【００３４】即ち、セキュリティレベルが設定された通信を行うサーバ装置２０及びクライアント装置３０が設けられたネットワーク通信システムにおいて、前記サーバ装置２０は、セキュリティレベル制御装置１０を有する。そして、このセキュリティレベル制御装置１０は、セキュリティレベル認識部１１及びセキュリティレベル設定部１４を備えて構成されている。

【００３５】（セキュリティレベル認識部１１）前記セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。

【００３６】（セキュリティレベル設定部１４）前記セキュリティレベル設定部１４は、前記セキュリティレベル認識部１１で認識されたセキュリティレベルを前記サーバ装置２０側のセキュリティレベルとして設定する。

【００３７】本発明の第２のネットワーク通信システムによれば、サーバ装置２０側において、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識されたクライアント装置３０のセキュリティレベルがサーバ装置２０側のセキュリティレベルとして設定される。

【００３８】《本発明の第３のネットワーク通信システム》本発明の第３のネットワーク通信システムは、前述した第１の課題を解決するため以下のように構成されている（請求項５に対応）。

【００３９】即ち、第１のネットワーク通信システムにおいて、前記サーバ装置２０は複数設けられている。そして、前記クライアント装置３０に設けられた前記セキュリティレベル制御装置１０は、各々のサーバ装置２０毎にセキュリティレベルを制御する。

【００４０】本発明の第３のネットワーク通信システムによれば、下記の作用が行われる。、即ち、各々のサーバ装置２０毎にセキュリティレベルが制御される。

《本発明の第４のネットワーク通信システム》本発明の第４のネットワーク通信システムは、前述した第１の課題を解決するため以下のように構成されている（請求項６に対応）。

【００４１】即ち、第２のネットワーク通信システムにおいて、前記クライアント装置３０は複数設けられている。そして、前記サーバ装置２０に設けられた前記セキュリティレベル制御装置１０は、各々のクライアント装置３０毎にセキュリティレベルを制御する。

【００４２】本発明の第４のネットワーク通信システムによれば、下記の作用が行われる。即ち、各々のクライアント装置３０毎にセキュリティレベルが制御される。

《本発明の第５のネットワーク通信システム》本発明の第５のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項７に対応）。

【００４３】即ち、第１又は第３のネットワーク通信システムにおいて、前記クライアント装置３０が有する前記セキュリティレベル制御装置１０は、セキュリティレベル変換テーブル部１２及びセキュリティレベル読出部１３を有する。

【００４４】セキュリティレベル変換テーブル部１２は、２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【００４５】セキュリティレベル読出部１３は、前記セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及び前記クライアント装置３０側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部１２から読み出す。

【００４６】そして、前記セキュリティレベル設定部１４は、前記セキュリティレベル読出部１３から読み出されたセキュリティレベルを前記クライアント装置３０側のセキュリティレベルとして設定する。

【００４７】本発明の第５のネットワーク通信システムによれば、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識されたサーバ装置２０のセキュリティレベル及びクライアント装置３０のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部１２から読み出される。そして、この読み出されたセキュリティレベルがクライアント装置３０側のセキュリティレベルとして設定される。

【００４８】《本発明の第６のネットワーク通信システム》本発明の第６のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項８に対応）。

【００４９】即ち、第２又は第４のネットワーク通信システムにおいて、前記サーバ装置２０が有する前記セキュリティレベル制御装置１０は、セキュリティレベル変換テーブル部１２及びセキュリティレベル読出部１３を

有する。

【００５０】セキュリティレベル変換テーブル部１２は、２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【００５１】セキュリティレベル読出部１３は、前記セキュリティレベル認識部１１で認識された前記クライアント装置３０のセキュリティレベル及び前記サーバ装置２０側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部１２から読み出す。

【００５２】そして、前記セキュリティレベル設定部１４は、前記セキュリティレベル読出部１３から読み出されたセキュリティレベルを前記サーバ装置２０のセキュリティレベルとして設定する。

【００５３】本発明の第６のネットワーク通信システムによれば、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識されたクライアント装置３０のセキュリティレベル及びサーバ装置２０側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部１２から読み出される。そして、この読み出されたセキュリティレベルがサーバ装置２０側のセキュリティレベルとして設定される。

【００５４】《本発明の第７のネットワーク通信システム》本発明の第７のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項９に対応）。

【００５５】即ち、第５のネットワーク通信システムにおいて、前記クライアント装置３０が有する前記セキュリティレベル制御装置１０は、前記クライアント装置３０の要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【００５６】本発明の第７のネットワーク通信システムによれば、下記の作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

《本発明の第８のネットワーク通信システム》本発明の第８のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項１０に対応）。

【００５７】即ち、第６のネットワーク通信システムにおいて、前記サーバ装置が有する前記セキュリティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【００５８】本発明の第８のネットワーク通信システムによれば、下記の作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

《本発明の第９のネットワーク通信システム》本発明の第９のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項１１に対応）。図５は、第９のネットワーク通信システムに対応した原理ブロック図である。

【００５９】即ち、セキュリティレベルが設定された通信を行うサーバ装置２０及びクライアント装置３０が設けられたネットワーク通信システムにおいて、前記サーバ装置２０及び前記クライアント装置３０は、セキュリティレベル制御装置１０を有する。このセキュリティレベル制御装置１０は、セキュリティレベル認識部１１、セキュリティレベル変換テーブル部１２、セキュリティレベル読出部１３及びセキュリティレベル設定部１４を備えて構成されている。

【００６０】（セキュリティレベル認識部１１）前記セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。

【００６１】（セキュリティレベル変換テーブル部１２）前記セキュリティレベル変換テーブル部１２は、２組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【００６２】（セキュリティレベル読出部１３）前記セキュリティレベル読出部１３は、前記セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置１０側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部１２から読み出す。

【００６３】（セキュリティレベル設定部１４）前記セキュリティレベル設定部１４は、前記セキュリティレベル読出部１３から読み出されたセキュリティレベルをセキュリティレベル制御装置１０側のセキュリティレベルとして設定する。

【００６４】本発明の第９のネットワーク通信システムによれば、下記の作用が行われる。まず、セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置１０側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部１２から読み出される。そして、この読み出されたセキュリティレベルがセキュリティレベル装置１０側のセキュリティレベルとして設定される。

【００６５】《本発明の第１０のネットワーク通信システム》本発明の第１０のネットワーク通信システムは、前述した第２の課題を解決するため以下のように構成されている（請求項１２に対応）。

【００６６】即ち、第９のネットワーク通信システムにおいて、前記クライアント装置３０が有する前記セキュリティレベル制御装置１０は、前記クライアント装置３０の要求に従って、通信途中でも、セキュリティレベル

を動的に変化させる。

【００６７】そして、前記サーバ装置２０が有する前記セキュリティレベル制御装置１０は、前記サーバ装置２０からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【００６８】本発明の第１０のネットワーク通信システムによれば、下記の作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

【００６９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

（実施形態のシステム構成）実施形態のシステムは、図６に示すように、サーバ装置２０（サーバとも言う）、このサーバ装置に接続されたネットワーク４０、及び、このネットワーク４０に接続されたクライアント装置３０（クライアントともいう）を備えて構成されている。

【００７０】このシステムでは、サーバ装置２０とクライアント装置３０との間で通信が行われる。この通信では、盗聴、改竄、なりすまし等を防止するため、通信内容の重要性に応じて５段階のセキュリティレベルを設定することが可能となっている。

【００７１】なお図６では、サーバ装置２０は１台しか示されていないが、複数台設けてもよい。同様に、クライアント装置３０は、図６では１台しか示されていないが、複数台設けてもよい。

【００７２】（セキュリティレベル）サーバ装置２０及びクライアント装置３０は、通信開始時に、それぞれ独立に設定したセキュリティレベルを相手に通知する。その後、サーバ装置２０及びクライアント装置３０は、互いのセキュリティレベルに基づいて定められるセキュリティレベルに従って通信する。

【００７３】本実施形態では、前述したように、５段階のセキュリティレベルを設定可能であるが、それらのセキュリティレベルは以下のようになる。

セキュリティレベル“１”：暗号化も認証も行わない。いわゆる普通の通信である。

【００７４】

セキュリティレベル“２”：暗号化だけを行う。

セキュリティレベル“３”：暗号化とユーザ認証を行う。

セキュリティレベル“４”：暗号化とサーバ認証を行う。なお、このセキュリティレベル“４”は、セキュリティレベル“３”と同等のセキュリティレベルである。

【００７５】

セキュリティレベル“５”：暗号化、ユーザ認証及びサーバ認証を行う。

なお、サーバ装置２０は、クライアント装置３０が複数設けられている場合に、個々のクライアント装置３０毎に独立したセキュリティレベルに従って通信することが可能である。

【００７６】また、クライアント装置３０は、サーバ装置２０が複数設けられている場合に、個々のサーバ装置２０毎に独立したセキュリティレベルに従って通信することが可能である。

【００７７】そして、セキュリティレベルとしては、他に次のようなものを設定することも可能である。即ち、セキュリティレベル“２”～“５”で暗号化を行わないもの、クライアントを認証するもの等である。

【００７８】さらに、ここでいうユーザ認証には、パスワードを用いた認証や公開鍵証明書を用いた認証が含まれる。本実施形態では、公開鍵証明書を用いた認証について説明する。

【００７９】（サーバ装置２０の構成）サーバ装置２０は、ネットワーク４０に接続された通信制御部２１、この通信制御部２１に接続されたサービス処理部２２、このサービス処理部２２に接続されたセキュリティレベル制御装置１０、及びサービス処理部２２に接続された記憶部２３を備えて構成されている。

【００８０】通信制御部２１は、サーバ装置２０がネットワーク４０との間で通信を行うための制御を行う。サービス処理部２２は、サーバ装置２０内で発生するさまざまなサービス要求を実現するため、セキュリティレベル制御装置１０、通信制御部２１及び記憶部２３との間でデータのやりとりを行う。

【００８１】記憶部２３は、ユーザの秘密鍵（SKm：mは添字）、ユーザの証明書（CERTm：mは添字）及び発行局の証明書（CERTca：caは添字）に関する情報を格納する。この記憶部２３は、例えば、ＲＡＭ（Random Access Memory）、半導体記憶装置、磁気ディスク記憶装置、磁気テープ装置、Ｍ／Ｏ（Magnet Optical：光磁気ディスク装置）、Ｉ／Ｃカード等が用いられる。

【００８２】セキュリティレベル制御装置１０は、通信開始時にクライアント装置３０から通知されたセキュリティレベルと、サーバ装置２０自体のセキュリティレベルとに基づいて、実際に行われる通信のセキュリティを制御する装置である。セキュリティレベル制御装置１０の構成については、クライアント装置３０の構成に続いて説明する。

【００８３】（クライアント装置３０の構成）クライアント装置３０は、ネットワーク４０に接続された通信制御部３１、この通信制御部３１に接続されたサービス処理部３２、このサービス処理部３２に接続されたセキュリティレベル制御装置１０、及びサービス処理部３２に接続された記憶部３３を備えて構成されている。

【００８４】通信制御部３１は、サーバ装置２０がネットワーク４０との間で通信を行うための制御を行う。サービス処理部３２は、クライアント装置３０内で発生するさまざまなサービス要求を実現するため、セキュリティレベル制御装置１０、通信制御部３１及び記憶部３３との間でデータのやりとりを行う。

【００８５】記憶部３３は、サーバの公開鍵（PKs：sは添字）、サーバの証明書（CERTs：sは添字）、サーバの秘密鍵（SKs：sは添字）及び発行局の証明書（CERTca：caは添字）に関する情報を格納する。この記憶部３３は、例えば、ＲＡＭ（Random Access Memory）、半導体記憶装置、磁気ディスク記憶装置、磁気テープ装置、Ｍ／Ｏ（Magnet Optical；光磁気ディスク）装置、ＩＣカード等が用いられる。

【００８６】セキュリティレベル制御装置１０は、通信開始時にサーバ装置２０から通知されたセキュリティレベルと、クライアント装置３０自体のセキュリティレベルとの折り合いをつける装置である。

【００８７】（セキュリティレベル制御装置１０の構成）サーバ装置２０に設けられたセキュリティレベル制御装置１０及びクライアント装置３０に設けられたセキュリティレベル制御装置１０は、同様に構成されているので、以下、両者を区別せずにその構成を説明する。

【００８８】セキュリティレベル制御装置１０は、図７に示すように、制御部１６、セキュリティレベル認識部１１、セキュリティレベル変換テーブル部１２、セキュリティレベル設定部１４、セキュリティレベル通知部１５、暗号処理部１７及び認証処理部１８を備えて構成されている。

【００８９】制御部１６は、サービス処理部２２（サーバ装置２０の場合）又はサービス処理部３２に接続（クライアント装置３０の場合）に接続されるとともに、セキュリティレベル認識部１１、セキュリティレベル変換テーブル部１２、セキュリティレベル読出部１３、セキュリティレベル設定部１４、セキュリティレベル通知部１５、暗号処理部１７及び認証処理部１８に接続されている。そして、制御部１６は、各部間のデータのやりとりを制御する。

【００９０】セキュリティレベル認識部１１は、通信先が通知してくるセキュリティレベルを認識する。セキュリティレベル変換テーブル部１２は、ネットワークで使用される全サーバ及び全クライアントがとりうるセキュリティレベルを１～５の５段階とした場合に、どのサーバ、クライアントでも該テーブルを使用可能とするために、サーバのインデックスを１～５とするとともに、クライアントのインデックスを１～５としている。そして、セキュリティレベル変換テーブル部１２は、実際に通信を行うサーバ、クライアントがそれぞれ要求するセキュリティレベルに基づき、計２５のパターンの中からいずれか１つが得られるように構成されている。

【００９１】図８には、本実施形態のセキュリティレベル変換テーブル部１２が示されている。同図の場合、例えば、クライアントのセキュリティレベルが“2”で、サーバのセキュリティレベルが“4”ならば、実際に行われる通信のセキュリティレベルは“4”となる。なお、“×”となっている部分は、サーバ装置２０及びクライアント装置３０がそれぞれ設定したセキュリティレベルでは、通信が行えないことを意味する。即ち、セキュリティレベルを制御できない場合に相当する。

【００９２】このように本実施形態のセキュリティレベル変換テーブル部１２は、サーバが提供する情報を重要と考え、クライアントが要求するセキュリティレベルよりもサーバが要求するセキュリティレベルの方が高い場合に、サーバが要求するセキュリティレベルを優先するようなテーブルとして構成されている。

【００９３】しかしながら、セキュリティレベル変換テーブル部１２の構成はこれに限るものではなく、自装置が要求できるセキュリティレベルのみを第１のインデックスとし、かつ、相手装置がとりうる全セキュリティレベルを第２のインデックスとしてテーブルを構成してもよい。例えば、上述のネットワークにおいて、自装置がクライアントで、かつセキュリティレベルは１～３を要求することが可能であり、相手装置となるサーバがとりうるセキュリティレベルが１～５とすると、自装置のインデックス（３個）×サーバのインデックス（５個）＝計１５個のパターンのなかからいずれか一つが得られるようにすればよい。

【００９４】セキュリティレベル読出部１３は、セキュリティレベル認識部１１で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置１０側のセキュリティレベルをインデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部１２から読み出す。

【００９５】セキュリティレベル設定部１４は、セキュリティレベル読出部１３から読み出されたセキュリティレベルをセキュリティレベル制御装置１０側のセキュリティレベルとして設定する。

【００９６】セキュリティレベル通知部１５は、自分のセキュリティレベルを通信先に通知する。暗号処理部１７は、通信先に出力するメッセージを暗号化したり、逆に、通信先から入力された暗号化済みのメッセージを復号化する。なお、本実施形態では、慣用鍵暗号方式（共通鍵方式）としてＤＥＳ(Data Encryption Standard)方式が用いられており、また、公開鍵暗号方式としてＲＳＡ方式(Rivest-Shamir-Aldeman) が用いられている。

【００９７】認証処理部１８は、サーバ認証を行ったり（クライアント装置３０の場合）、ユーザ認証を行ったりする。

（実施形態におけるクライアント装置３０及びサーバ装置２０間の処理シーケンス）次に、図９及び図１０を参照して、実施形態におけるクライアント装置３０及びサーバ装置２０間の処理シーケンス例を説明する。なお、ここで説明する処理シーケンスは、その全てが実行されるわけではなく、セキュリティレベル毎に必要な部分のみ実行される。

【００９８】まず、クライアント装置３０は、サーバ装

置２０に通信要求を通知する（ステップ９０１。この通知を(1)で表す）。この通信要求に対して、サーバ装置２０は、クライアント装置３０にアクセプトを通知する（ステップ９０２。この通知を(2)で表す）。

【００９９】クライアント装置３０にアクセプトが通知された後、クライアント装置３０及びサーバ装置２０間で、通信の前処理が行われる（ステップ９０３。この前処理を(3)で表す）。ここで、通信の前処理とは、例えば、端末型情報、表示方法情報（何行、何桁で表示するか）、使用文字コード種別情報、ＩＰアドレス等の情報交換を行うことをいう。

【０１００】通信の前処理が終了した後、クライアント装置３０は、クライアント装置３０が設定したセキュリティレベルをサーバ装置２０に通知する（ステップ９０４。この通知を(4)で表す）。この通知により、サーバ装置２０は、クライアント装置３０が設定したセキュリティレベルを認識する（ステップ９０５。この認識を(6)で表す）。

【０１０１】続いて、サーバ装置２０は、サーバ装置２０が設定したセキュリティレベルをクライアント装置３０に通知する（ステップ９０６。この通知を(5)で表す）。この通知により、クライアント装置３０は、サーバ装置２０が設定したセキュリティレベルを認識する（ステップ９０７。この認識を(7)で表す）。

【０１０２】クライアント装置３０は、クライアント装置３０側で設定したセキュリティレベルとサーバ装置２０から通知されたセキュリティレベルに従って、実際に行われる通信のセキュリティレベルを選択する（ステップ９０８。この選択を(8)で表す）。また、サーバ装置２０は、サーバ装置２０側で設定したセキュリティレベルとクライアント装置３０から通知されたセキュリティレベルに従って、実際に行われる通信のセキュリティレベルを選択する（ステップ９０９。この選択を(8)で表す）。

【０１０３】ここで、ステップ９０８及びステップ９０９で選択されるセキュリティレベルは、互いに一致する。その後、クライアント装置３０は、ユーザの証明書(CERTm) をサーバ装置２０に通知する（ステップ９１０。この通知を(A)で表す）。

【０１０４】サーバ装置２０は、通知されたユーザの証明書を発行局の証明書(CERTca)で検証する（ステップ９１１）。また、サーバ装置２０は、サーバの公開鍵（PKs） 又はサーバの証明書(CERTs)をクライアント装置３０に通知する（ステップ９１２。この通知を(B)で表す）。

【０１０５】クライアント装置３０は、通知されたサーバの証明書(CERTs) を発行局の証明書(CERTca)で検証する（ステップ９１３）。また、クライアント装置３０は、認証（ここでは、サーバの認証）を行う種であるDEK1を乱数により生成する（ステップ９１４）。

【０１０６】その後、クライアント装置３０は、サーバの公開鍵(PKs) でDEK1を暗号化することにより生成したPKs(DEK1) をサーバ装置２０に通知する（ステップ９１５。この通知を(C)で表す）。つまり、発信者であるクライアント装置３０は、本文を読むための共通の暗号鍵（共通鍵）を、受信者であるサーバ装置２０の公開鍵(PKs) で暗号化して通知する。ここまでの処理段階では、クライアント装置３０及びサーバ装置２０に共通の暗号鍵（共通鍵）が無いため、暗号化は、公開鍵暗号方式（ＲＳＡ方式）で行われる。

【０１０７】サーバ装置２０は、通知されたPKs(DEK1) をサーバの秘密鍵(SKs) で復号化することによりDEK1を取り出す（ステップ９１６）。つまり、受信者であるサーバ装置２０は、自分の秘密鍵であるサーバの秘密鍵(SKs) で共通鍵を復号化する。その後、クライアント装置３０から送られる本文は、復号された共通鍵で復号化される。

【０１０８】また、サーバ装置２０は、サーバの秘密鍵(SKs) を用いてDEK1を行うことによりSKs(DEK1) を生成する（ステップ９１７）。その後、サーバ装置２０は、SKs(DEK1) をDEK1で暗号化することにより生成したDEK1(SKs(DEK1)) をクライアント装置３０に通知する（ステップ９１８。この通知を(D)で表す）。ここで、SKs(DEK1) をDEK1で暗号化するのは、電子署名を盗聴されないためである。また、電子署名は、発信者（ユーザ）の認証と本文内容に改竄が行われていないことを検証するために行われる。例えば、署名者Ａは、適切な関数を使って本文のダイジェストを作り、それをＡの秘密鍵を用いて暗号化する。これが署名となる。検証者Ｂは、署名者Ａの公開鍵を用いて署名を元に戻し、その結果が原本の本文のダイジェストに等しいかを調べる。等しくなければ、本文は改竄されていることが分かる。

【０１０９】ここで、クライアント装置３０は、処理Ｐとして、以下の１）～３）を行う（ステップ９１９）。１）DEK1(SKs(DEK1)) を復号化してSKs(DEK1) を取り出す。２）取り出されたSKs(DEK1) からサーバの証明書の中の公開鍵(PKs) を用いて、DEK1を取り出す。３）取り出されたDEK1とステップ９１４で生成されたDEK1とを比較する。この比較により、サーバの認証が行われることになる。この認証が行われるのは、サーバの証明書として公開されている鍵が本当にサーバ装置２０のものかどうかを確認するためである。この確認は、第三者機関が認証するサーバの証明書(CERTs) を用いて行われる。このような確認は、第三者認証あるいは電子公証人とも呼ばれている。簡単に言うと、自分が送ったものに対し相手に署名をしてもらい、その署名を相手の公開鍵でほどした結果が自分の送ったものと同一であれば、認証ができたことになるということである。

【０１１０】クライアント装置３０は、ステップ９１９の３）の比較の結果、同じであればサーバ装置２０にAC

K を通知し、異なっていればサーバ装置２０にNACKを通知する（ステップ９２０）。

【０１１１】次に、サーバ装置２０は、認証（ここでは、ユーザの認証）を行う種であるDEK2を乱数により生成する（ステップ９２１）。その後、サーバ装置２０は、慣用暗号化方式を用いてDEK2を暗号化することにより生成したDEK1(DEK2)をクライアント装置３０に通知する（ステップ９２２。この通知を(F)で表す）。ここで、慣用暗号化方式が用いられる理由は、クライアント装置３０及びサーバ装置２０に暗号鍵DEK1が共有化されていることと、その暗号鍵DEK1を用いると処理速度が速くなるためである。いいえかれば、すべてを公開鍵で行うと計算量が膨大になることに原因して処理速度が落ちるのを防ぐためである。

【０１１２】次に、クライアント装置３０は、サーバ装置２０から通知されたDEK1(DEK2)をユーザの秘密鍵(SKm) で復号化することによりDEK2を取り出す（ステップ９２３）。

【０１１３】また、クライアント装置３０は、ユーザの秘密鍵(SKm) を用いてDEK2に対して電子署名を行うことによりSKm(DEK2) を生成する（ステップ９２４）。その後、クライアント装置３０は、SKm(DEK2) をDEK2で暗号化することにより生成したDEK2(SKm(DEK2)) を通知する（ステップ９２５。この通知を（G）で表す）。

【０１１４】ここで、サーバ装置２０は、処理Qとして、以下の１）～３）を行う（ステップ９２６）。１）DEK2(SKm(DEK2)) を復号化してSKm(DEK2) を取り出す。２）取り出されたSKm(DEK2) からユーザの秘密鍵(SKm) を用いてDEK2を取り出す。３）取り出されたDEK2とステップ９２１で生成されたDEK2とを比較する。この比較により、ユーザの認証が行われることになる。

【０１１５】サーバ装置２０は、ステップ９２６の３）の比較の結果、同じであればクライアント装置３０にACK を通知し、異なっていればクライアント装置３０にNACKを通知する（ステップ９２７。この通知を(H)で表す）。

【０１１６】その後、クライアント装置３０及びサーバ装置２０間で、暗号鍵DEK2を用いた通信が行われる（ステップ９２８。この通信を（９）で表す）。

（各セキュリティレベルで行われる処理シーケンス）次に、各セキュリティレベルで行われる処理シーケンスを図１１を参照して説明する。

【０１１７】まず、セキュリティレベル“１”では、前述した（１）、（２）、（３）、（４）、（５）、（６）、（７）、（８）及び（９）の動作が順に処理が行われる。

【０１１８】また、セキュリティレベル“２”では、前述した（１）、（２）、（３）、（４）、（５）、（６）、（７）、（８）、（Ｂ）、（Ｃ）及び（Ｆ）の動作が順に処理が行われる。

【０１１９】そして、セキュリティレベル“３”では、前述した（１）、（２）、（３）、（４）、（５）、（６）、（７）、（８）、（Ａ）、（Ｂ）、（Ｃ）、（Ｆ）、（Ｇ）及び（Ｈ）の動作が順に処理が行われる。

【０１２０】そして、セキュリティレベル“４”では、前述した（１）、（２）、（３）、（４）、（５）、（６）、（７）、（８）、（Ｂ）、（Ｃ）、（Ｄ）、（Ｅ）及び（Ｆ）の動作が順に処理が行われる。

【０１２１】そして、セキュリティレベル“５”では、前述した（１）、（２）、（３）、（４）、（５）、（６）、（７）、（８）、（Ａ）、（Ｂ）、（Ｃ）、（Ｄ）、（Ｅ）、（Ｆ）、（Ｇ）及び（Ｈ）の動作が順に処理が行われる。

【０１２２】（処理動作例その１）次に、図１２を参照して、処理動作例その１の処理動作を説明する。まず、クライアント装置３０（クライアント）が通信先にアクセスする（ステップ１２０１）。

【０１２３】次に、サーバ装置２０（サーバ）がクライアントの通信をアクセプトする（ステップ１２０２）。ここで、通信の前処理が完了する（ステップ１２０３）。

【０１２４】次に、クライアントがセキュリティレベル“３”を要求する（ステップ１２０４）。この要求により、サーバのセキュリティレベル制御装置１０は、クライアントのセキュリティレベルを“３”と認識する（ステップ１２０５）。

【０１２５】次に、サーバがセキュリティレベル“５”を要求する（ステップ１２０６）。この要求により、クライアントのセキュリティレベル制御装置１０は、サーバのセキュリティレベルを“５”と認識する（ステップ１２０７）。

【０１２６】ここで、サーバ及びクライアントのセキュリティレベル制御装置１０は、セキュリティレベル変換テーブル部１２に従って、セキュリティレベル“５”を選択する（ステップ１２０８）。

【０１２７】サーバ及びクライアントは、図９及び図１０の（Ａ）、（Ｂ）、（Ｃ）、（Ｄ）、（Ｅ）、（Ｆ）、（Ｇ）及び（Ｈ）の処理シーケンスと暗号鍵の交換を実行した後、暗号化通信を行う（ステップ１２０９）。

【０１２８】（処理動作例その２）次に、図１３を参照して、処理動作例その２の処理動作を説明する。まず、クライアント装置３０（クライアント）が通信先にアクセスする（ステップ１３０１）。

【０１２９】次に、サーバ装置２０（サーバ）がクライアントの通信をアクセプトする（ステップ１３０２）。ここで、通信の前処理が完了する（ステップ１３０３）。

【０１３０】次に、クライアントがセキュリティレベル

“２”を要求する（ステップ１３０４）。この要求により、サーバのセキュリティレベル制御装置１０は、クライアントのセキュリティレベルを“２”と認識する（ステップ１３０５）。

【０１３１】次に、サーバがセキュリティレベル“２”を要求する（ステップ１３０６）。この要求により、クライアントのセキュリティレベル制御装置１０は、サーバのセキュリティレベルを“２”と認識する（ステップ１３０７）。

【０１３２】ここで、サーバ及びクライアントのセキュリティレベル制御装置１０は、セキュリティレベル変換テーブル部１２に従って、セキュリティレベル“２”を選択する（ステップ１３０８）。

【０１３３】サーバ及びクライアントは、図９及び図１０の（Ｂ）、（Ｃ）及び（Ｆ）の処理シーケンスと暗号鍵の交換を実行した後、暗号化通信を行う（ステップ１３０９）。

【０１３４】（本実施形態の効果）以上説明したように、本実施形態では、相手装置の要求レベルだけに基づいて通信のレベルを決めるのではなく、双方の装置の要求レベルにより実際の通信のレベルを決めるようにしたため、以下のような効果を生じる。即ち、インターネットに本実施例を適用した場合に、サーバとユーザの装置（インターネットの世界ではホストと呼ばれる）間で通信を行う場合に、サーバは、提供する情報を暗号化して他の装置に参照させないようにしたいのに対し、ユーザが平文での通信を要求するような場合でも、セキュリティレベル変換テーブル部１２を、サーバの要求レベルが優先されるように構成しておくことで、問題が生じるようなことがなくなる。

【０１３５】

【発明の効果】本発明の第１のセキュリティレベル制御装置及び第１から第４のネットワーク通信システムによれば、セキュリティレベル認識部で認識されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するようにしたので、通信先との間で予めセキュリティレベルを決定しておくことなく通信を行うことを可能となる。

【０１３６】本発明の第２のセキュリティレベル制御装置及び第５から第１０のネットワーク通信システムによれば、通信先から通知されたセキュリティレベルと、セキュリティレベル制御装置が設けられる側のセキュリティレベルとに基づいて、セキュリティレベルを設定するようにしたので、自分のセキュリティレベルを反映させた通信を行うことを可能となる。

【図面の簡単な説明】

【図１】本発明の第１のセキュリティレベル制御装置に対応した原理ブロック図である。

【図２】本発明の第２のセキュリティレベル制御装置に対応した原理ブロック図である。

【図３】本発明の第１のネットワーク通信システムに対応した原理ブロック図である。

【図４】本発明の第２のネットワーク通信システムに対応した原理ブロック図である。

【図５】本発明の第９のネットワーク通信システムに対応した原理ブロック図である。

【図６】実施形態のシステム構成図である。

【図７】実施形態のセキュリティレベル制御装置の構成ブロック図である。

【図８】実施形態のセキュリティレベル制御装置が有するセキュリティレベル変換テーブル部を示す図である。

【図９】実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その１）を示す図である。

【図１０】実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その２）を示す図である。

【図１１】実施形態の各セキュリティレベルで行われる処理シーケンスを示す図である。

【図１２】実施形態における処理動作例その１の処理フローチャートを示す図である。

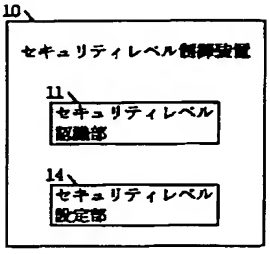
【図１３】実施形態における処理動作例その２の処理フローチャートを示す図である。

【符号の説明】

１０・・・セキュリティレベル制御装置（セキュリティレベル制御部）
１１・・・セキュリティレベル認識部
１２・・・セキュリティレベル変換テーブル
１３・・・セキュリティレベル読出部
１４・・・セキュリティレベル設定部
１５・・・セキュリティレベル通知部
１６・・・制御部
１７・・・暗号処理部
１８・・・認証処理部
２０・・・サーバ装置
３０・・・クライアント装置
３１・・・通信制御部
３２・・・サービス処理部
３３・・・記憶部
４０・・・ネットワーク

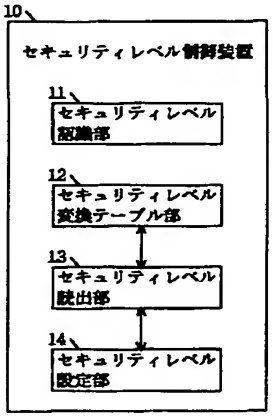
【図１】

本発明の第１のセキュリティレベル制御装置に対応した原理ブロック図



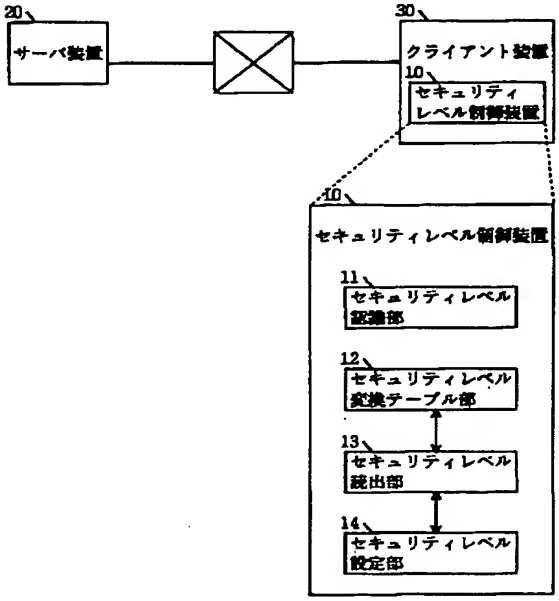
【図２】

本発明の第２のセキュリティレベル制御装置に対応した原理ブロック図



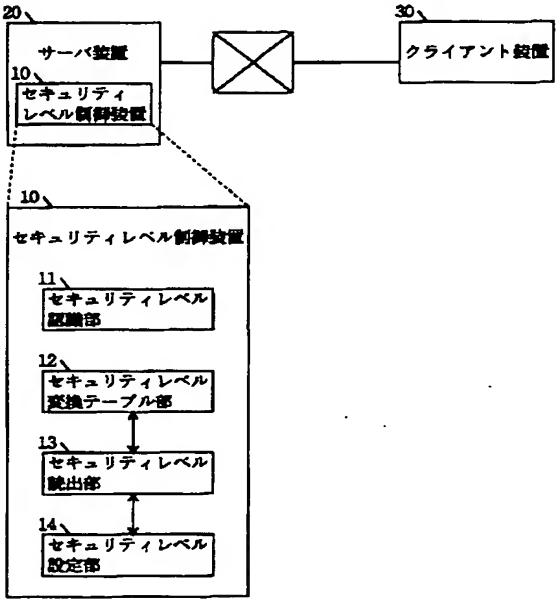
【図３】

本発明の第１のネットワーク通信システムに対応した原理ブロック図



【図４】

本発明の第２のネットワーク通信システムに対応した原理ブロック図



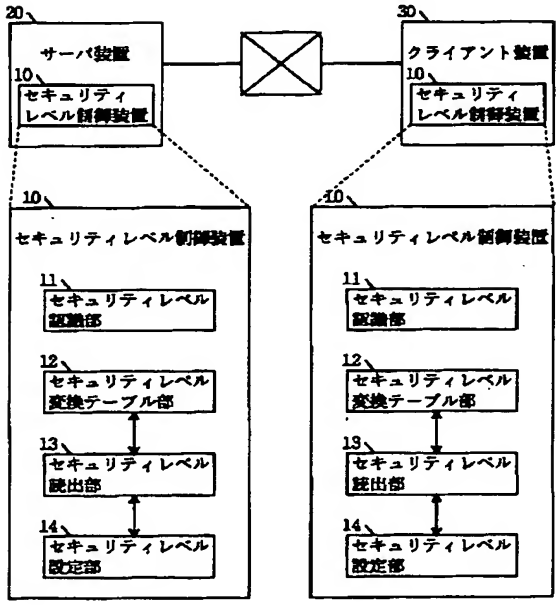
【図８】

実施形態のセキュリティレベル制御装置が有する
セキュリティレベル変換テーブル部を示す図

クライアントのセキュリティレベル ＼ サーバのセキュリティレベル	1	2	3	4	5
1	1	2	×	4	×
2	2	2	×	4	×
3	×	2	3	×	5
4	×	×	×	4	×
5	×	×	×	4	5

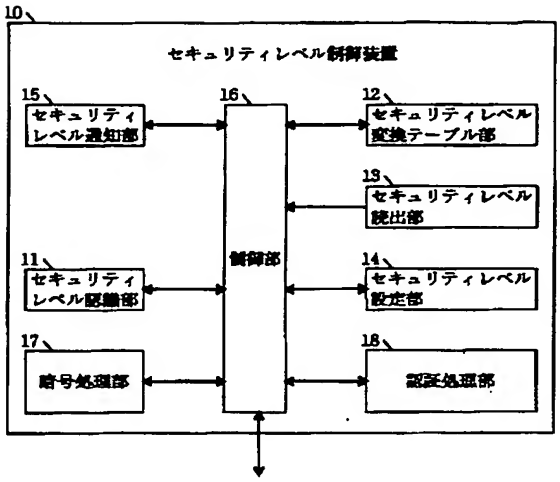
【図５】

本発明の第９のネットワーク通信システムに対応した原理ブロック図



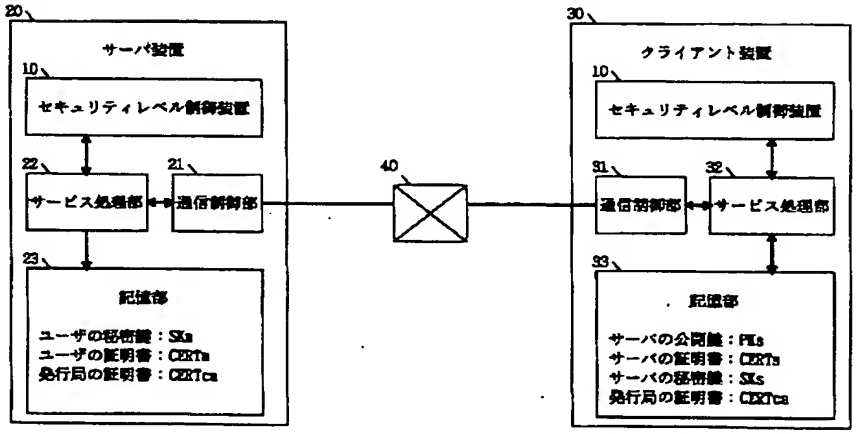
【図７】

実施形態のセキュリティレベル制御装置の構成ブロック図



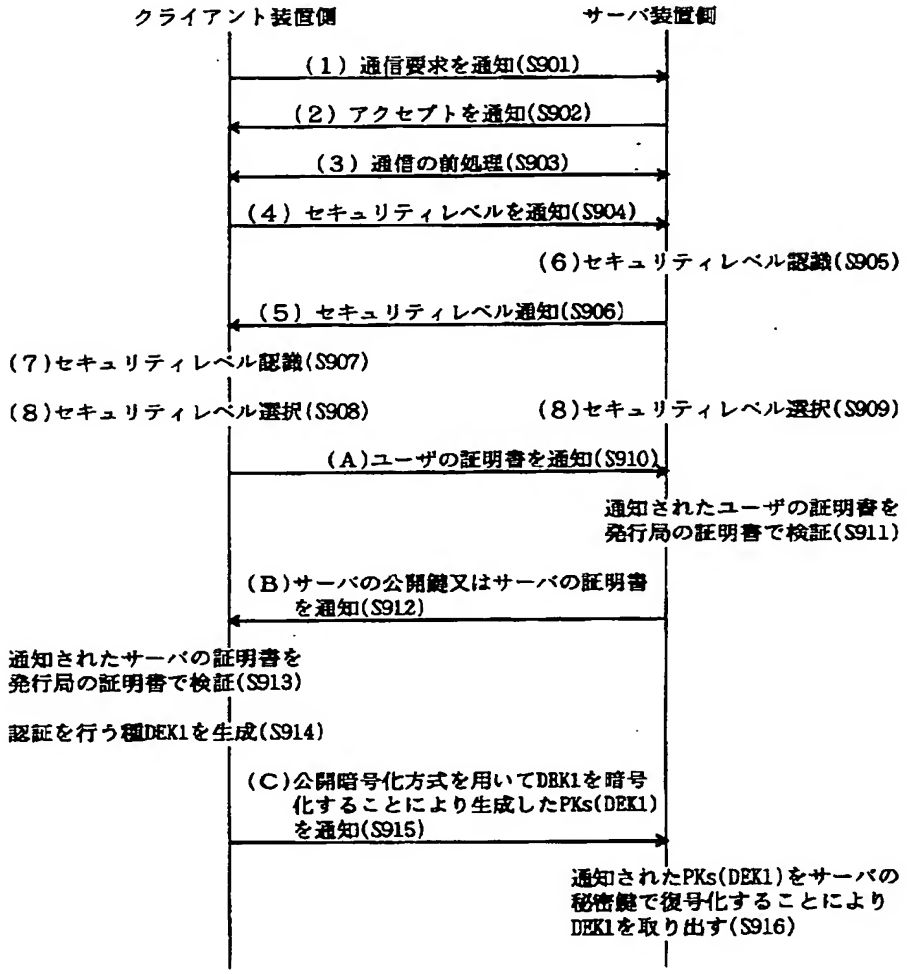
【図６】

実施形態のシステム構成図



【図９】

実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その１）



【図１１】

実施形態の各セキュリティレベルで行われる処理シーケンス

セキュリティ
レベル "1"　(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(9)

セキュリティ
レベル "2"　(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(F)

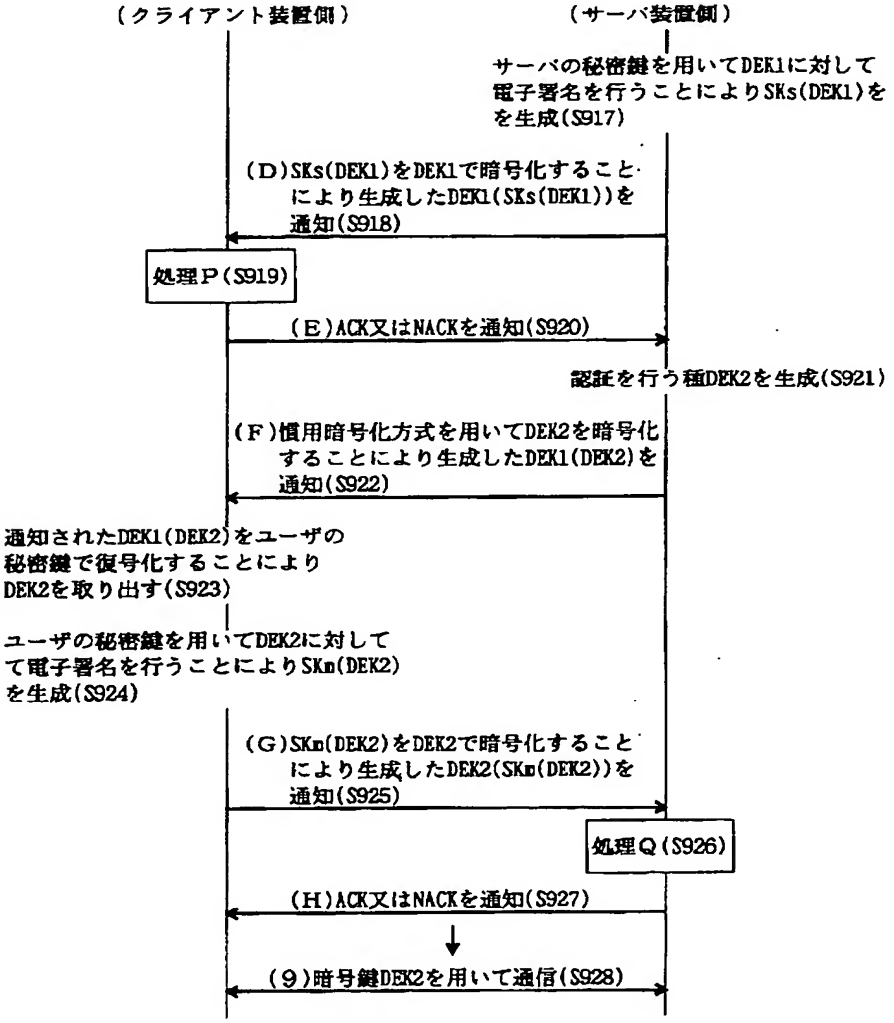
セキュリティ
レベル "3"　(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(F)→(G)→(H)

セキュリティ
レベル "4"　(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(D)→(E)→(F)

セキュリティ
レベル "5"　(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(D)→(E)→(F)→(G)→(H)

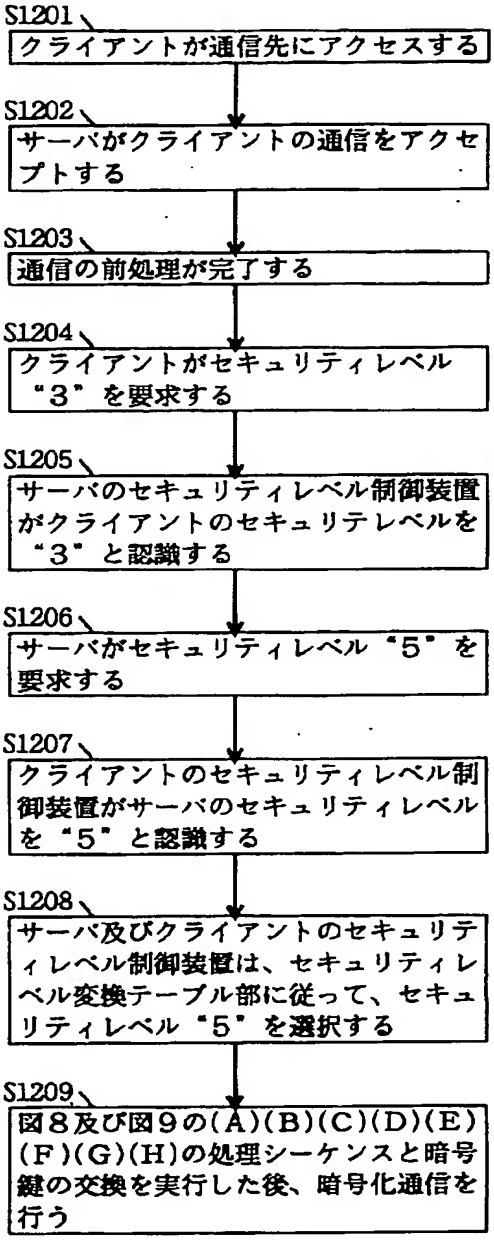
【図１０】

実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その２）



【図１２】

実施形態における処理動作例その１の処理フローチャート



【図１３】

実施形態における処理動作例その２の処理フローチャート